

The Fermat curve $x^n + y^n + z^n$: the most symmetric non-singular algebraic plane curve

F. Pambianco

Abstract. A non-singular plane algebraic curve of degree n ($n \geq 4$) is called maximally symmetric if it attains the maximum order of the projective automorphism groups for non-singular plane algebraic curves of degree n .

Highly symmetric curves give rise to extremely good error-correcting codes and are ideal for the construction of good universal hash families and authentication codes (see [2], [3], [4], [5]).

In this work it is proven that the maximally symmetric non-singular plane curves of degree n in \mathbf{P}^2 ($n \notin \{4, 6\}$) are projectively equivalent to the Fermat curve $x^n + y^n + z^n$. For some particular values of $n \leq 20$ the result has been obtained in [9], [15], [16], [19]. As to the two exceptional cases, $n = 4, 6$, it is known that the Klein quartic [11] and the Wiman sextic [8] are respectively the uniquely determined maximally symmetric curves.

0 Introduction

Algebraic curves play an important role in the study of error-correcting codes. Nearly 30 years have passed since V. Goppa discovered an ingenious method to construct error-correcting codes from an algebraic curve [22]. The automorphism group of an algebraic curve is one of its important invariants. The questions of deriving upper bounds on orders and of constructing curves with particularly large automorphism groups have always been considered as particularly important. Landmark papers in this direction are the celebrated Hurwitz bound, Stichtenoth's thesis [20], the theorem by Valentini-Madan [23] and the construction of the Deligne-Lusztig curves [7]. There is a general tendency that highly symmetric curves have extremal behaviour also in other respects. They tend to have a large number of rational points and are, therefore, ideally suited for the construction of good error-correcting codes; besides they tend to have Weierstrass points with large gaps [21]. A popular example is the Klein quartic. Its automorphism group meets the Hurwitz bound, it yields the maximal possible number of rational places over suitable fields and it also has Weierstrass points with exotic gap distribution. Another surprising area of application of highly symmetric curves is the theory of universal hashing and authentication in computer science as introduced by Carter and Wegman [6]. For the underlying theory and description of various applications see [2], [3], [4], [5]. It turns out that the characteristics mentioned earlier are precisely what is needed for the construction of good

universal hash families and authentication codes.

Therefore it is natural to ask what are the non-singular plane algebraic curves of degree n ($n \geq 4$) which attain the maximum order of the projective automorphism groups for non-singular plane algebraic curves of degree n .

In this paper k stands for an algebraically closed field k of characteristic 0. In the projective plane \mathbf{P}^2 over k , let $V(f)$ denote the projective irreducible curve associated with a non-constant homogeneous polynomial $f(x, y, z) \in k[x, y, z]$. By a classical result dating back to 19th century, the automorphism group $\text{AUT}(f)$ of $V(f)$ is finite provided that $V(f)$ is neither rational or elliptic. For curves of genus $g \geq 2$, the Hurwitz upper bound on the size of $\text{AUT}(f)$ is $84(g - 1)$. Assume that $V(f)$ is non-singular. Then $g = (n - 1)(n - 2)/2$ where $n = \deg f$. If $n \geq 4$ then $\text{AUT}(f)$ is the group $\text{Aut}(f)$ of all projectivities of \mathbf{P}^2 which leave $V(f)$ invariant. Moreover, Hurwitz's bound reads $|\text{AUT}(f)| \leq 42n(n - 3)$. It should be noted that Hurwitz's bound is not attainable for many values of n . This leads to the following definition. A non-singular curve $V(f)$ of degree n ($n \geq 4$) is called *maximally symmetric* if $\text{Aut}(f)$ attains the maximum size of the (projective) automorphism groups of non-singular plane algebraic curves of degree n .

The main result of this paper is the following theorem:

Theorem 1 *Assume that $n \geq 8$. Let f be a non-singular plane algebraic curve of degree n in \mathbf{P}^2 . Then $|\text{Aut}(f)| \leq 6n^2$, where equality holds if and only if f is projectively equivalent to $x^n + y^n + z^n$.*

In other words, for $n \geq 8$, the Fermat curve is, up to a projectivity, the unique maximally symmetric non-singular plane curve of degree n . Actually, this remains true for every $n < 8$ except for the two cases, namely $n = 4$ and $n = 6$. It is known that the Klein quartic (as we have said above) and the Wiman sextic [25] are maximally symmetric for $n = 4$ [11] and $n = 6$ [8], respectively. As for the automorphism group and related geometry of the Wiman sextic, see [14]. Since non-singular curves of degree $n = 1$ or $n = 2$, are unique up to projectivities, they are equivalent to $x^n + y^n + z^n$. For cubic curves, see [19] and [9]. The case of prime degree $n \leq 20$ was investigated in [15], [16]. Surveys on automorphism groups of algebraic curves are found in [10], [1] and [12, Chapter 11].

1 Preliminaries

A finite group H in $PGL(2, \mathbf{C})$ is isomorphic to \mathbf{A}_5 , \mathbf{S}_4 , \mathbf{A}_4 , $\mathbf{D}_{2\nu}$ ($\nu \geq 2$), or \mathbf{Z}_ν ($\nu \geq 1$) ([24], [13]).

Lemma 1.1 *Let k and k' be algebraically closed fields of characteristic zero. If K is a finite subgroup of $PGL(n, k)$ with $n \geq 2$, then there exists a finite subgroup K' of $PGL(n, k')$ such that $K \cong K'$. In particular a finite group of $PGL(2, k)$ is isomorphic to \mathbf{A}_5 , \mathbf{S}_4 , \mathbf{A}_4 , $\mathbf{D}_{2\nu}$ ($\nu \geq 2$), or \mathbf{Z}_ν ($\nu \geq 1$).*

Proof. Let $\rho_k : SL(n, k) \rightarrow PSL(n, k) = PGL(n, k)$ be the standard surjective group homomorphism. Clearly $\text{Ker } \rho_k = \{\zeta^\ell E_n ; i \in [1, n]\}$, where ζ is a primitive n -th root of unity. Assume $K = \{(A_j) ; j \in [1, |K|]\}$, where $A_j \in SL(n, k)$. By Brauer's theorem a finite

subgroup of $GL(n, k)$ is conjugate to a finite subgroup of $GL(n, \overline{\mathbf{Q}})$ [17, p.487]. Thus there exists a $T \in SL(n, k)$ such that $T\rho_k^{-1}(K)T^{-1} = \{\zeta^\ell TA_j T^{-1} ; j \in [1, |K|], \ell \in [1, n]\}$, where $TA_j T^{-1} \in SL(n, \overline{\mathbf{Q}})$. We may assume $\tilde{K} = T\rho_k^{-1}(K)T^{-1} \subset SL(n, k')$. Now $\rho_{k'}(\tilde{K})$ is isomorphic to K .

Lemma 1.2 *For $\alpha, \varepsilon, \eta \in k^*$ with $\text{ord}(\varepsilon) = e$, $\text{ord}(\eta) = h$ and $\alpha^e \in \langle \eta \rangle$ let $A = \text{diag}[\alpha\varepsilon, \alpha]$ and $C = \eta E_2$. Then the order of the group $K = \langle A, C \rangle$ is eh .*

Proof. We may assume $e, h \geq 2$. Assume $\alpha^e = \eta^m$ with $m \in [1, h]$, and let $m = m'c$ and $h = h'c$, where $c = \text{gcd}(m, h)$. It can be shown easily that $\text{ord}(A) = eh' = eh/c$. The map $\chi : \langle A \rangle \times \langle C \rangle \rightarrow K$ sending (X, Y) to XY is a surjective group homomorphism. It suffices to show that $|\text{Ker } \chi| = h/c$. $A^i C^j$ with $(i, j) \in [1, eh'] \times [0, h-1]$ belongs to $\text{Ker } \chi$ if and only if $i = ei'$ ($i' \in [1, h']$) and $mi' + j = 0 \pmod{h}$. There are exactly $h' = h/c$ such (i, j) .

For $A = [a_{ij}] \in GL(n, k)$ with $A^{-1} = [\alpha_{ij}]$ we associate a transformation T_A of $k[x] = k[x_1, \dots, x_n]$ by $T_A f(x) = f_A(x) = f(\sum_{i=1}^n \alpha_{1i} x_i, \dots, \sum_{i=1}^n \alpha_{ni} x_i)$. Then $f_{AB} = (f_B)_A$ for $f \in k[x]$ and $A, B \in GL(n, k)$. Thus $T_{AB} = T_A T_B$ so that T_A is a bijection of $k[x]$.

Lemma 1.3 *If a non-zero $f \in k[x]$ satisfies $f_A = \lambda f$ ($\lambda \in k^*$), and $\text{ord}(A) = \nu < \infty$, then $\lambda^\nu = 1$.*

Proof. Since $f = f_{A^\nu} = (f_A)_{A^{\nu-1}} = \lambda^\nu f$, we get $(\lambda^\nu - 1)f = 0$.

Lemma 1.4 [16] *Let $f_1, \dots, f_n \in k[x]$ be non-zero homogeneous polynomials of the same degree such that $f_{jA} = \lambda_j f_j$ ($j = 1, 2, \dots, n$) for an $A \in GL(3, k)$ with mutually distinct λ_j . Then a linear combination $f = c_1 f_1 + \dots + c_n f_n \neq 0$ satisfies $f_A = \lambda f$ for some $\lambda \in k$ if and only if $c_j \neq 0$ except for just one value of j .*

Let ε be a primitive n -th root of 1 ($n \geq 3$). A cyclic subgroup of order n in $PGL(3, k)$ clearly is conjugate to either $G_{0,1} = \langle (\text{diag}[1, 1, \varepsilon]) \rangle$ or $G_{i,j} = \langle (\text{diag}[1, \varepsilon^i, \varepsilon^j]) \rangle$ for some $1 \leq i < j \leq n-1$ satisfying $\text{gcd}(i, j, n) = 1$.

2 The main theorem

The finite subgroups of $PGL(3, k)$ have been classified [18, Theorem 1–Theorem 16]. If G does not leave invariant a point, a line or a triangle, then $|G|$ belongs to $\{36, 72, 168, 360\}$ so that $|G| < 6n^2$ for $n \geq 8$. We will describe finite groups G of the following types: leaving invariant either a point or a line; permuting cyclically the vertices of a triangle; permuting the vertices of a triangle as S_3 .

Let π_2 be the canonical homomorphism from $GL(2, k)$ onto $PGL(2, k)$ such that $\pi_2(B) = (B)$. We introduce a notation to denote an element of $GL(3, k)_{[0,0,1]} = \{A \in GL(3, k) ; A[0, 0, 1] = [0, 0, 1]\}$. For $A' = [a'_{ij}] \in GL(2, k)$ and $a' = [a'_1, a'_2] \in k^2$ $[A', a']$ stands for the matrix $A = [a_{ij}] \in GL(3, k)$ such that $a_{ij} = a'_{ij}$, $a_{3j} = a'_j$ ($j \in [1, 2]$), $a_{i3} = 0$ ($i \in [1, 2]$), and $a_{33} = 1$. Let $PGL(3, k)_{(0,0,1)} = \{(A) \in PGL(3, k) ; (A) \text{ fixes } (0, 0, 1)\}$. Then the map $\tau : PGL(3, k)_{(0,0,1)} \rightarrow GL(3, k)_{[0,0,1]}$ sending (A) to A/a_{33} is a group isomorphism, where $A = [a_{ij}]$. Denote by π the map sending $[A', a'] \in GL(3, k)_{[0,0,1]}$ to $A' \in GL(2, k)$, and let $\psi = \pi_2 \circ \pi$. Let G_1 and G_2 be subgroups of $PGL(3, k)_{(0,0,1)}$. Then they are conjugate in $PGL(3, k)_{(0,0,1)}$, if and only if $\tau(G_1)$ and $\tau(G_2)$ are conjugate in $GL(3, k)_{[0,0,1]}$. If they are conjugate in $PGL(3, k)_{(0,0,1)}$, then $\psi(\tau(G_1))$ and $\psi(\tau(G_2))$ are conjugate in $PGL(2, k)$.

Proposition 2.1 *Assume that a finite subgroup G_0 of $PGL(3, k)$ leaves the point $(0, 0, 1)$ invariant. Then G_0 is conjugate to some G in $PGL(3, k)_{(0,0,1)}$ with the following properties. Let $G' = \tau(G)$, $G'' = G' \cap \text{Ker } \psi$ and $H = \psi(G')$. Then G'' is a cyclic group generated by a matrix $\text{diag}[\eta, \eta, 1]$, where $\text{ord}(\eta) = |G|/|H|$.*

- (1) *If H is isomorphic to \mathbf{A}_5 , \mathbf{S}_4 , or \mathbf{A}_4 , then $|G''| > n$, provided $|G| \geq 6n^2$ with $n \geq 11$.*
- (2) *If H is isomorphic to $\mathbf{D}_{2\nu}$ ($\nu \geq 2$), then there exist $\alpha, \varepsilon, \eta \in k^*$ such that*

$$G' = \langle \text{diag}[\alpha\varepsilon, \alpha, 1], \text{diag}[\eta, \eta, 1], [\theta e_2, \theta e_1, e_3] \rangle,$$

where $\theta \in \{1, \sqrt{\eta}\}$, $\text{ord}(\varepsilon) = \nu$, $\text{ord}(\eta) = |G''|$ with $\alpha^\nu, \alpha^2\varepsilon \in \langle \eta \rangle$. If $|G''| = 1$, then ν is odd, and $\alpha = \varepsilon^i$ with $i = (\nu - 1)/2$ and $\theta = 1$. Let $G'_d = \langle \text{diag}[\alpha\varepsilon, \alpha, 1], \text{diag}[\eta, \eta, 1] \rangle$. Then $G' = G'_d + G'_d[\theta e_2, \theta e_1, e_3]$ with $|G'_d| = \nu|G''|$.

- (3) *If H is isomorphic to \mathbf{Z}_ν , then there exists $\alpha \in k^*$ such that $\alpha^\nu \in \langle \varepsilon \rangle$,
 $G' = \langle \text{diag}[\alpha\varepsilon, \alpha, 1], \text{diag}[\eta, \eta, 1] \rangle$, where $\text{ord}(\varepsilon) = \nu$, and $|G'| = \nu|G''|$.*

A finite subgroup G of $PGL(3, k)$ leaving the line z invariant is conjugate to a finite subgroup $\{(B)|(^tB) \in G\}$ where a finite subgroup G of $PGL(3, k)$ fixes the point $(0, 0, 1)$.

Proposition 2.2 *Let G be a finite subgroup of $PGL(3, k)$ permuting cyclically the vertices of a triangle. Then G is conjugate to a group*

$$\langle (\text{diag}[\alpha\varepsilon, \alpha, 1]), (\text{diag}[\eta, \eta, 1]), ([e_3, e_1, e_2]) \rangle,$$

where $\text{ord}(\varepsilon) = \nu$, $\text{ord}(\eta) = \mu$, $\alpha^\nu \in \langle \eta \rangle$, and $|G| = 3\nu\mu$.

Theorem 2.3 *Let G be a finite subgroup of $PGL(3, k)$ with $|G| \geq 6n^2$ and $f(x, y, z)$ a non-zero homogeneous polynomial of degree $n \geq 11$ which is G -invariant. If G leaves invariant the point $(0, 0, 1)$ or the line z or G is as described in Proposition 3.2 then f is singular.*

Proposition 2.4 *Let G be a finite subgroup of $PGL(3, k)$ inducing \mathbf{S}_3 on the vertices of the triangle $\triangle P_1P_2P_3$, where $P_1 = (1, 0, 0)$, $P_2 = (0, 1, 0)$ and $P_3 = (0, 0, 1)$. Denote by G_0 the isotropy group at $P_3 = (0, 0, 1)$. Then G has the following form up to conjugation.*

$$\begin{aligned} G &= G_0 + G_0([e_3, e_1, e_2]) + G_0([e_3, e_1, e_2])^2 \text{ with} \\ G_0 &= \langle (\text{diag}[\alpha\varepsilon, \alpha, 1]), (\text{diag}[\eta, \eta, 1]), ([\beta e_2, \gamma e_1, e_3]) \rangle, \end{aligned}$$

where $\alpha, \beta, \gamma, \varepsilon, \eta \in k^*$. Let $G'_0 = \tau(G_0)$, $G'_{0,d} = \langle \text{diag}[\alpha\varepsilon, \alpha, 1], \text{diag}[\eta, \eta, 1] \rangle$, and $H = \psi(G'_0)$. H is isomorphic to \mathbf{Z}_ν ($\nu \geq 1$) or $\mathbf{D}_{2\nu}$ ($\nu \geq 2$).

If $H \simeq \mathbf{Z}_\nu$, then $\varepsilon = \alpha = 1$, $\nu = 2$, $\beta\gamma \in \langle \eta \rangle$, $\text{ord}(\eta) = \mu$, $|G_0| = 2\mu$ and $|G| = 6\mu$.

If $H \simeq \mathbf{D}_{2\nu}$, then $\text{ord}(\varepsilon) = \nu$, $\text{ord}(\eta) = \mu$, $\{\alpha^\nu, \beta\gamma\} \subset \langle \eta \rangle$, $|G_0| = 2\nu\mu$ and $|G| = 6\nu\mu$.

Theorem 2.5 *Let G be a finite subgroup of $PGL(3, k)$ described in Proposition 2.4 with $|G| \geq 6n^2$. Let $f(x, y, z)$ be a homogeneous polynomial of degree $n \geq 11$. Then a G -invariant f is non-singular, if and only if G is conjugate to*

$$\tilde{G} = \langle (\text{diag}[\varepsilon, 1, 1]), (\text{diag}[1, 1, \varepsilon]), ([e_2, e_1, e_3]), ([e_3, e_1, e_2]) \rangle,$$

where $\text{ord}(\varepsilon) = n$. The \tilde{G} -invariant f is equal to $x^n + y^n + z^n$ up to constant multiplication.

Proof. (sketch) Assume that f is G -invariant and of degree n .

1) If H is isomorphic to \mathbf{Z}_2 , then G contains $(\text{diag}[1, 1, \eta])$ with $\text{ord}(\eta) = \mu \geq n^2 > n$, hence f is singular.

2) Assume $H \simeq \mathbf{D}_{2\nu}$. G contains a subgroup $G_{0,d} = \langle (A), (C) \rangle$, where $A = [\text{diag}[\alpha\varepsilon, \alpha, 1]$ and $C = \text{diag}[1, 1, \eta]$ with $\text{ord}(\varepsilon) = \nu$, $\text{ord}(\eta) = \mu$ and $\alpha^\nu \in \langle \eta \rangle$. Note $\nu\mu = |G|/6 \geq n^2$.

3) Only for $\mu = n$ and $\nu = n$ f is not singular. In this case $f = ax^n + by^n + cz^n$ ($a, b \in k^*$).

4) f is projectively equivalent to $f' = x^n + y^n + z^n$ and consequently $|G| = 6n^2$.

This completes the proof of the following main theorem:

Theorem 2.6 *If $n \geq 11$, then the most symmetric non-singular plane algebraic curve of degree n is projectively equivalent to $x^n + y^n + z^n$.*

3 The case where the degree is between 8 and 10

The main theorem remains valid for $n = 8, 9, 10$. This is a corollary of the following three propositions in which statements and proofs it is of great importance the following famous

Theorem 3.1 (Hurwitz) *Denote by $\text{AUT}(C)$ the automorphism group of a projective non-singular irreducible algebraic curve C of genus $g \geq 2$. Let $g' = g - 1$. The possible sizes of $\text{AUT}(C)$ at least $12g'$ are*

$$\frac{12m}{m-6} g'$$

where $m \in \{s \in \mathbf{Z}; s \geq 7\} \cup \{8 + \frac{4}{7}, 16 + \frac{4}{5}, \infty\}$.

Let $f(x, y, z)$ be a homogeneous polynomial of degree n .

Proposition 3.2 *Let $n = 8$.*

(1) *If f is either \mathbf{Z}_5 -invariant or \mathbf{Z}_{11} -invariant, then f is singular.*

(2) *Let G be a subgroup of $PGL(3, k)$ with $|G| = 2^7$. If f is non-singular and G -invariant, then f is projectively equivalent to $x^n + y^n + z^n$.*

Proposition 3.3 *Let $n = 9$ and let G be a finite subgroup of $PGL(3, k)$.*

- (1) *Let $|G| = 2^3$. Then G is isomorphic to one of \mathbf{Z}_8 , $\mathbf{Z}_4 \times \mathbf{Z}_2$, \mathbf{D}_8 or \mathbf{Q}_8 . Let f be G -invariant. If f is non singular then G is isomorphic to \mathbf{Z}_8 and $|\text{Aut}(f)| < 6n^2$.*
- (2) *If $|G| = 3^3$, then G is isomorphic to one of \mathbf{Z}_{27} , $\mathbf{Z}_9 \times \mathbf{Z}_3$ and \mathbf{E}_{27} , where $\mathbf{E}_{27} = \langle a, b ; a^3 = b^3 = [a, b]^3 = 1, [[a, b], a] = [[a, b], b] = 1 \rangle$ with $[a, b] = a^{-1}b^{-1}ab$. A \mathbf{Z}_{27} -invariant f is singular.*
- (3) *If a non-singular f with $|\text{Aut}(f)| \geq 6n^2$ is either $\mathbf{Z}_9 \times \mathbf{Z}_3$ -invariant or \mathbf{E}_{27} -invariant, then f is projectively equivalent to $x^n + y^n + z^n$.*

Proposition 3.4 *Let $n = 10$.*

- (1) *If f is \mathbf{Z}_7 -invariant, \mathbf{Z}_{13} -invariant or \mathbf{Z}_{25} -invariant, then f is singular.*
- (2) *If f is non-singular and $\mathbf{Z}_5 \times \mathbf{Z}_5$ -invariant, then f is projectively equivalent to $x^n + y^n + z^n$.*

Corollary 3.5 *Propositions 3.2, 3.3 and 3.4 imply respectively that Theorem 2.5 holds for $n = 8, 9, 10$.*

References

- [1] R.D.M. Accola, *Topics in the Theory of Riemann Surfaces*, Lecture Notes in Math. **1595**, Springer Verlag 1994.
- [2] J. Bierbrauer, Universal hashing and geometric codes, *Designs, Codes and Cryptography* **11** (1997), 207-221.
- [3] J. Bierbrauer, *Introduction to Coding Theory*, Chapman and Hall/CRC Press 2005.
- [4] J. Bierbrauer, Authentication via algebraic-geometric codes, in Recent Progress in Geometry, *Supplemento ai Rendiconti del Circolo Matematico di Palermo* **51** (1998), 139-152.
- [5] J. Bierbrauer, T.Johansson, G.Kabatiansky, B.Smeets, On families of hash functions via geometric codes and concatenation, *Proceedings CRYPTO 93, Lecture Notes in Computer Science* **773** (1994), 331-342.
- [6] J.L. Carter and M. N. Wegman, Universal classes of hash functions, *J. Computer and System Sci.* **18** (1979), 143-154.
- [7] P. Deligne and G. Lusztig, Representations of reductive groups over finite fields, *Annals of Mathematics* **103** (1976), 103-161.
- [8] H. Doi, K. Idei and H. Kaneta, Uniqueness of the most symmetric non-singular plane sextics, *Osaka J. Math.* **37** (2000), 667-687.
- [9] F. Enriques and O. Chisini, *Teoria Geometrica delle Equazioni delle Funzioni Algebriche, I-IV*, Bologna, Zanichelli, 1915-1934.
- [10] H. M. Farkas and I. Kra, *Riemann Surfaces, 2nd edition*, Springer, 1992.

- [11] R. Hartshorne, *Algebraic Geometry*, Springer, 1977.
- [12] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, *Algebraic Curves over a Finite Field*, Princeton Univ. Press, Princeton and Oxford, 2008.
- [13] S. Iitaka, *Algebraic Geometry II (in Japanese)*, Iwanami, 1977.
- [14] H. Kaneta, S. Marcugini and F. Pambianco, On arcs and curves with many automorphisms, *Mediterranean J. Math.* **2** (2005), 71–102.
- [15] H. Kaneta, S. Marcugini and F. Pambianco, The most symmetric non-singular plane curves of degree $n < 8$, *RIMS Kokyuroku* **1109** (1999), 182–191.
- [16] H. Kaneta, S. Marcugini and F. Pambianco, The most symmetric non-singular plane curves of degree $n \leq 20$, I, *Geom. Dedicata* **85** (2001), 317–334.
- [17] S. Lang, *Algebra*, Addison-Wesley, 1965.
- [18] H. H. Mitchell, Determination of the ordinary and modular ternary linear groups, *Trans. Amer. Math. Soc.* **12** (1911), 207–242.
- [19] J. G. Semple and G. T. Kneebone, *Algebraic Curves*, Oxford Clarendon Press, 1959.
- [20] H. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik, *Arch. Math* **24** (1973), 527-544 and 615-631.
- [21] H. Stichtenoth, *Algebraic function fields and codes*, Second Edition, Springer 2009.
- [22] M. Tsfasman, S. Vladut and D. Nogin, *Algebraic Geometric Codes: Basic Notions*, AMS, 2007.
- [23] R.C. Valentini and M.L. Madan, A hauptsatz of L.E. Dickson and Artin-Schreier extensions, *J. Reine und Angew. Math.* **318** (1980), 156-177.
- [24] H. Weber, *Lehrbuch der Algebra*, 2^{te} Auflage, Vieweg Verlag, 1899.
- [25] A. Wiman, Übere eine einfache Gruppe von 360 ebenen Collineationen, *Math. Annalen* **47**(1896), 531–556.